3331	What is the HIPAA Administrative Simplification Compliance Act (ASCA)?	In December 2001, the Administrative Simplification Compliance Act (ASCA) extended the deadline for compliance with the HIPAA Electronic Health Care Transactions and Code Sets standards (codified at 45 C.F.R. Parts 160, 162) one year to October 16, 2003 for all covered entities other than small health plans (whose compliance date was already October 16, 2003). In order to receive an extension, covered entities must submit their ASCA compliance plans on or before October 15, 2002 ASCA requires that a sample of the plans will be provided to the National Committee on Vital and Health Statistics (NCVHS), an advisory committee to the Secretary of Health and Human Services. The NCVHS will review the sample to identify common problems that are complicating compliance activities, and will periodically publish recommendations for solving the problems. Under the Freedom of Information Act (FOIA), information held by the federal government is available to the public on request, unless it falls within one of several exemptions. The model form is designed to avoid collection of any information that would be subject to exemption, such as confidential personal or proprietary information. If such information is submitted, both the FOIA and the ASCA require that it be redacted before the files are released either to the NCVHS or to the public. For additional information regarding HIPAA, please visit “http://cms.hhs.gov/hipaa/".
3382	How does the ASCA delay affect Medicare implementation activities?	Medicare will continue to implement the HIPAA transaction standards on a sequenced basis, and that schedule will not change significantly. We expect to be ready to test the claim and several other transactions by Spring 2002, but implementation of several transactions (such as the referral/authorization transaction) will be in early FY 2003. Once a provider has successfully tested a transaction with us, it will be able to use the standard in our production environment.
3403	Why didn’t Congress just give everyone an ASCA extension?	The requirement to submit a compliance extension plan provides assurance that covered entities have plans in place that will allow them to be compliant by the new deadline of October 16, 2003.
3414	Is HHS going to actually review & approve all ASCA compliance plans?	Submission of a properly completed compliance extension plan is sufficient to secure the one-year extension.
3535	When will Medicaid Agencies test ASCA compliant transactions with trading partners?	Each Medicaid State Agency has its own project plan for achieving HIPAA compliance, and will decide whether to submit a compliance plan. If you are a trading partner, you will receive notice of testing directly from the Medicaid State Agency(s) with whom you do business.
3546	Does the law require Medicare claims to be submitted electronically after Oct. 2003?	ASCA prohibits HHS from paying Medicare claims that are not submitted electronically after October 16, 2003, unless the Secretary grants a waiver from this requirement. It further provides that the Secretary must grant such a waiver if there is no method available for the submission of claims in electronic form or if the entity submitting the claim is a small provider of services or supplies. Beneficiaries will also be able to continue to file paper claims if they need to file a claim on their own behalf. The Secretary may grant such a waiver in other circumstances. We will publish proposed regulations to implement this new authority.
928	Are small providers exempt	The term “small providers” originates in the Administrative Simplification Compliance Act (ASCA), the law

7	from HIPAA?	which requires those providers/submitters who bill Medicare to begin submitting only electronic claims to Medicare on October 16, 2003 in the HIPAA format. However, ASCA does provide an exception to the Medicare electronic claims submission requirements to "small providers". ASCA defines a small provider or supplier as: a provider of services with fewer than 25 full-time equivalent employees or a physician, practitioner, facility or supplier (other than a provider of services) with fewer than 10 full-time equivalent employees. It is important to keep in mind that this provision does not preclude providers from submitting paper claims to other health plans. In addition, if a provider transmits any of the designated transactions electronically, it is subject to the HIPAA Administrative Simplification requirements regardless of size.
9318	Can you provide a definition of testing, and does it relate to all transactions?	ASCA requires that testing begin no later than April 2003. The law itself did not specify what type of testing, (e.g. internal, external, final with trading partners, all transactions, or just one, etc.) HHS interprets this to mean the date requested on the extension form as the date when internal system testing begins for the first transaction the covered entity will test. However, some covered entities will need to begin their external testing sooner than others, especially those that have many trading partners or are implementing many of the transactions. We encourage all covered entities to begin testing as soon as possible.
11839	How should a health plan determine what receipts to use to decide whether it qualifies as a 'small health plan?'	A small health plan is defined at 45 C.F.R.§ 160.103 as "a health plan with annual receipts of $5 million or less." Health plans that report receipts to the IRS on identified tax forms. Health plans that file certain federal tax returns and report receipts on those returns should use the following guidance provided by the Small Business Administration at 13 C.F.R. § 121.104 to calculate annual receipts: Receipts means 'total income' (or in the case of a sole proprietorship, 'gross income') plus 'cost of goods sold' as these terms are defined or reported on Internal Revenue Service (IRS) Federal tax return forms; Form 1120 for corporations; Form 1120S for Subchapter S corporations; Form 1065 for partnerships; and Form 1040, Schedule F for farm or Schedule C for sole proprietorships). However, the term "receipts" excludes net capital gains or losses, taxes collected for and remitted to a taxing authority if included in gross or total income, proceeds from the transactions between a concern and its domestic or foreign affiliates (if also excluded from gross or total income on a consolidated return filed with the IRS), and amounts collected for another by a travel agent, real estate agent, advertising agent, conference management service provider, freight forwarder or customs broker. In calculating receipts under this guidance, health plans should use the definitions and process described at 13 C.F.R. § 121.104(a)(2) - (3) and § 121.104(b). Health plans that do not report receipts to the IRS on identified tax forms. Health plans that do not report receipts to the IRS – for example, ERISA group health plans that are exempt from filing income tax returns – should use proxy measures to determine their annual receipts. Fully insured health plans should use the amount of total premiums which they paid for health insurance benefits during the plan's last full fiscal year.
12121	How does the Small Business Administration definition change affect the HIPAA definition?	The Small Business Administration has changed its definition of a "small business concern" from an entity that receives less than $5 million in receipts annually to an entity that receives less than $6 million. This change does not affect the HIPAA definition. While HHS relied on advice from the Small Business Administration in developing its definition of a small health plan, it did not formally adopt the Small Business Administration

		definition as the definition for HIPAA purposes. For HIPAA purposes, a small health plan remains an entity that has receipts of $5 million or less per year.
121311	Should the premiums paid for stop-loss insurance be included in the amount of receipts?	The premiums or amounts paid for stop-loss insurance by an employer or sponsor of a self-insured plan should not be included in the amount of receipts.
128912	Is a fully insured ERISA plan a covered entity under HIPAA?	ERISA plans are covered in the definition of "health plan" and therefore are covered entities. The only exception is for ERISA plans that have less than 50 participants AND are self-administered. Fully insured ERISA plans therefore are HIPAA covered entities. The HIPAA statute gives "small health plans" an additional year to comply with the HIPAA standards. ERISA plans that meet the definition of a small plan do not need to submit an extension request, because they already have until October 16, 2003 to become compliant. A small plan is defined as having annual receipts of $5 million or less. Guidance on computing receipts is included in a frequently asked questions on our website (http://www.cms.hhs.gov/hipaa/hipaa2).
129013	Does CMS have free HIPAA billing software that non-Medicare providers can use to submit claims in the HIPAA format?	CMS has required Medicare contractors to upgrade their current free/low-cost Medicare claim billing software to comply with the requirements of the X12N 837 version 4010A1 claims format. This software allows creation of a HIPAA-compliant Medicare Part A or Part B claim. The software is designed to collect all of the 837 required data elements as well as those situational data elements that apply to Medicare. The software was not designed to enable billing of non-Medicare payers.
129114	What are the different adjudication requirements? Doesn't HIPAA mandate all electronic claims be standard?	HIPAA requires that all electronic claims be submitted in a standard format and comply with all required data elements and those situational data elements that are applicable based on the conditions described in the HIPAA implementation guide. HIPAA does not impact payers' coverage rules. The Medicare free billing software is being developed to support the submission of Medicare HIPAA compliant claims only. The software will not capture any of the situational data elements that may apply to other payers, but not to Medicare. For example, the professional HIPAA 837 implementation guide has fields for the service authorization exception code and immunization batch number. These are required by some Medicaid plans according to the law in those States. The Medicare free billing software will not include fields for that data since the information does not apply to Medicare. Another example is the repricing information in the 837. Repricers use this data, but the Medicare free billing software will not capture this information, since we do not reprice claims. In turn, the Medicare free billing software may provide for submission of certain situational data that may apply only to Medicare, such as Durable Medical Equipment (DME) data for the Medicare certificates of medical necessity (CMN).
129215	If a provider believes they can use the Medicare free/low cost software to bill payers other than Medicare, may	Yes, but providers who believe the Medicare free billing software also meets the needs of some other payer(s) are responsible for an in depth evaluation of the Medicare software to ascertain that each of another payer's applicable situational data elements are in fact captured by the Medicare software. They would probably need to test the software with the other payers to make a definitive determination. Medicare will not provide any

	they do so?	support in regard to problems encountered when a payer uses our software to bill another payer.
129316	Will the Medicare free/low cost software enable providers to be HIPAA compliant?	The software will allow providers to create a HIPAA-compliant claim for Medicare, however, there is no guarantee a non-Medicare payer will accept the claim, since situational data that applies to the other payer may be absent. To actually comply with the HIPAA requirements, however, providers must submit data when using the software that complies with the requirements in the 837-implementation guides. They must use the appropriate code sets, enter valid data that meets the minimum and maximum length requirements for a field, supply all required and otherwise applicable data, etc. Providers that do not submit appropriate, valid data will not be HIPAA compliant, even if they use the Medicare software to format their data in compliance with the 837 standard. Medicare does not require our contractors to supply software that supports the creation of HIPAA transactions other than the claim. Some may do so using a product developed by their corporate parent or if included in a commercial product that the contractor may have obtained to satisfy the Medicare requirement for free billing software, but this is not a Medicare requirement and contractor costs related to use of non-claim software are not reimbursable by Medicare. Providers that intend to use the other HIPAA transactions are expected to obtain their own software for this purpose, or contract with a third party such as a clearinghouse to provide the service on their behalf. Many payers find that use of a health care clearinghouse enables them to minimize the number of changes that must be made to their internal systems to support the HIPAA format requirements. At their option, providers may contract with a health care clearinghouse to reformat their data to meet HIPAA requirements. Of course, it is still the provider's responsibility to supply the clearinghouse with each of the data elements needed to allow the clearinghouse to produce compliant transactions.
129417	Does Medicare furnish any other type of free software?	Providers that receive electronic remittance advice (835 version 4010) transactions from Medicare will be offered free PC-Print software. This software can create a paper remittance advice from an 835 for use in billing of another payer or to create a version of the remittance advice that may be easier to read.
129518	We understand that Medicare will no longer offer free billing software after next year. Why?	The software was originally introduced as an incentive for providers to begin to bill Medicare electronically. Medicare has accepted electronic bills for more than 12 years, and was one of the first in the health care industry to do so. When we first had free billing software developed, there was little electronic billing software available that met Medicare's needs. In addition, the free software gave our providers an incentive to try billing electronically with minimal cost. Most of the early users of the free billing software overcame their initial suspicion of electronic data interchange and later migrated to more sophisticated software that could be used to bill multiple payers or that could also be used for practice management applications. With growing standardization across the health care industry, and a major increase in production and marketing of software to meet HIPAA transaction needs for the entire health care industry, we expect the rate of movement to alternate software products to accelerate in the future. In addition, with the increase in availability of commercial products and growing experience of provider staff with automated billing, there is less need for a government-supplied product that has limited application. However, if a significant volume of providers are still dependent on it, we will assess whether the free billing software should be continued.
1329	Who will enforce the HIPAA	The Department of Health and Human Services (HHS) has determined that CMS will have responsibility for

19	standards?	enforcing the transactions and code set standards, as well as security and identifiers standards when those are published. CMS will also continue to enforce the insurance portability requirements under Title I of HIPAA. The Office for Civil Rights in HHS will enforce the privacy standards.
1330 20	Doesn't the HIPAA law envision HHS providing technical assistance to the industry to help them become compliant?	Yes. Our enforcement strategy will concentrate on achieving voluntary compliance through technical assistance. Penalties would be imposed as a last resort.
1331 21	What will the enforcement process look like?	The enforcement process for HIPAA transactions and code sets (and for security and standard identifiers when those are adopted) will be primarily complaint-driven. Upon receipt of a complaint, CMS would notify the provider of the complaint, and the provider would have the opportunity to demonstrate compliance, or to submit a corrective action plan. If the provider does neither, CMS will have the discretion to impose penalties.
1332 22	What kinds of penalties could be imposed?	The Administrative Simplification Compliance Act (ASCA) permits the Secretary of HHS to exclude noncompliant covered entities from the Medicare program between October 16, 2002 and October 16, 2003 if they have not submitted an extension request. In addition, the original HIPAA legislation permits civil monetary penalties of not more than $100 for each violation, with a cap of $25,000 per calendar year. (Much larger penalties are provided for certain wrongful disclosure of individually identifiable health information). Thus, the ASCA penalty is for failure to submit an extension request, and it applies only to Medicare providers, while the HIPAA penalty is for noncompliance, and is generally applicable. Medicare providers could be both excluded and fined, while non-Medicare covered entities would be subject only to the civil monetary penalties.
1333 23	Will these penalties be imposed on all covered entities that did not submit requests?	No. The process leading to these penalties would be initiated primarily in response to an external complaint filed against a covered entity. Once a complaint is received, the entity will have opportunities to avoid penalties by demonstrating compliance, showing how they will achieve compliance by submitting a corrective action plan, or, for ASCA purposes, showing that they had submitted an extension request. Only when an entity does none of these things would consideration be given to invoking civil monetary penalties or excluding a provider from Medicare.
1336 24	What should a covered entity that did not submit an extension request do now?	They should come into compliance as soon as possible, and should be prepared to submit a corrective action plan in the event a complaint is filed against them.
1337 25	Will a covered entity that was not in existence prior to October 15, 2002 be subject to these penalties?	A newly formed covered entity could utilize a clearinghouse or compliant vendor to become compliant at the time it comes into existence. If the entity is not able to achieve compliance immediately, good faith efforts could be taken into account in the event a complaint is filed. Also, in the event of a complaint, the entity could submit a corrective action plan.
1468	Why have national standards	Congress and the health care industry have agreed that standards for the electronic exchange of administrative

26	for electronic health care transactions been adopted?	and financial health care transactions are needed to improve the efficiency and effectiveness of the health care system. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the Secretary of Health and Human Services to adopt such standards.
146927	What health care transactions are required to use the standards under HIPAA?	As required by HIPAA, the Secretary of Health and Human Services is adopting standards for the following administrative and financial health care transactions: □ Health claims and equivalent encounter information. □ Enrollment and disenrollment in a health plan. □ Eligibility for a health plan. □ Health care payment and remittance advice. □ Health plan premium payments. □ Health claim status. □ Referral certification and authorization. □ Coordination of benefits.
157228	I'm a provider who bills electronically. Do I have to implement the HIPAA if I go back to submitting claims on paper?	As a provider who bills electronically, you will be required to comply with the HIPAA requirements of the Privacy Rule by April 14, 2003, unless, before that date, you stop conducting any of the HIPAA transactions electronically. The HIPAA transactions commonly used by providers include claims, eligibility queries, claim status queries, and referrals. It is important to note that you cannot avoid the HIPAA requirements by hiring another entity, such as a billing service, to conduct these transactions electronically for you. While you and other health care providers could revert to conducting solely paper transactions, doing so would have many negative effects for most providers. The provider's business processes would be disrupted by having to prepare paper claims and check eligibility and claim status by phone. Reverting to paper would cause particular problems for those providers who receive Medicare payments. First, these providers would experience delays in receiving payments, because Medicare by law cannot pay paper claims until 28 days after receipt (as opposed to 14 days for electronic claims). Second, effective October 16, 2003, Medicare is prohibited by law from paying paper claims except for those from small providers and under certain other limited circumstances. After that date, any provider that does not meet the "small provider" or other exception would have to return to electronic claims submission in order to continue to receive Medicare reimbursement. At that time, the provider would again be required to comply with the Privacy Rule requirements.
178629	What is the covered entity status when a provider bills paper and a health plan converts a paper claim to electronic format?	Most, if not all, health plans transform the paper claims they receive into electronic formats for processing. The health plans do this for their own convenience, not on behalf of the providers submitting the paper claims. The provider described in the Question above would be a covered entity if its paper claims were submitted to a health care clearinghouse or a billing service, and, on behalf of the provider, that health care clearinghouse or the billing service transformed them into standard transactions and transmitted them to a health plan.

184730	How do I know whether to use the National Drug Code (NDC), the Healthcare Common Procedural Coding System (HCPCS), or another code set when reporting drugs and biologics transactions other than those with retail pharmacies?	The final rule adopting changes to the HIPAA Electronic Transactions and Code Set standards that was published in the Federal Register on February 20, 2003, does not adopt a standard. Therefore, it permits the use of any code set to allow current practices based upon business needs to continue. In the absence of an adopted standard medical data code set, the implementation guides adopted as HIPAA standards must be consulted. We will be working with the industry to expand the implementation guides to accommodate allowing additional code sets for reporting drugs and biologics on non-retail pharmacy drug transactions. If you currently use HCPCS to report drugs and biologics you may continue to do so. You may also use the NDC code set if you meet the conditions for use in the implementation guide. However, this modification does not alter the adopted NDC standard for reporting drugs and biologics on retail pharmacy transactions
184831	The Final Rule adopting changes to the HIPAA Electronic Transactions and Code Set Standards was published in the Federal Register on February 20, 2003 and adopts the Addenda as part of the standards for electronic transactions. With the adoption of the Addenda, should I be implementing ASC X12N 4010 or ASC X12N 4010A1?	The Addenda are not stand-alone documents. They are modifications to the implementation specifications for the initial standards adopted in the Transactions final rule of August 2000 and are not complete guides. The newly adopted standards, to be used by October 16, 2003 are the ASC X12N 4010 and the ASC X12N 4010A1 implementation guides.
184932	What is the purpose of and why were security standards needed as published in the Federal Register on February 20, 2003?	The purpose of this Security Standards rule is to adopt national standards for safeguards to protect the confidentiality, integrity, and availability of electronic protected health information. They were needed because there were no standard measures existing in the health care industry that addressed all aspects of the security of electronic protected health information while it is in use, in storage, or during the exchange of that information between entities. HIPAA mandated security standards to protect an individual's health information, while permitting the appropriate access and use of that information by health care providers, clearinghouses, and health plans.
185133	Do the Security Standards as published in the Federal Register on February 20, 2003 require use of specific technologies?	No. The Security standards were designed to be "technology neutral" in order to facilitate use of the latest and most promising technologies that meet the needs of different healthcare organizations. Any regulatory requirement for implementation of specific technologies would bind the health care community to specific systems and/or software that may be superseded by rapidly developing technologies and improvements.
185234	How could a small provider implement the security	The security standards regulation allows any covered entity (including small providers) to use any security measures that allow the covered entity to reasonably and appropriately implement the standards. In deciding

	standards as published in the Federal Register on February 20, 2003?	what security measures to use, a covered entity can take into account its size, capabilities, and costs of security measures. A small provider who is a covered entity would first assess their security risks and vulnerabilities and the mechanisms currently in place to mitigate those risks and vulnerabilities. Following this assessment, they would determine what additional measures, if any, need to be taken to meet the standards; taking into account their capabilities and the cost of those measures.
185335	Is HHS going to create and publish a list of Federally "certified" security software and off-the-shelf products?	While HHS will not produce such a list of security software and off-the-shelf products, it should be pointed out that other Government agencies such as the National Institute of Standards and Technology (NIST) are working towards that end. The health care industry is encouraged to monitor the activity of NIST and provide comments and suggestions when requested (see http://www.niap.nist.gov.).
185436	Why is there not a mandatory requirement to use encryption for transmissions over the Internet?	There remain significant financial and technical burdens associated with using encryption tools. Particularly when considering situations faced by small and rural providers, it is clear that there is not yet available a simple and interoperable solution to encrypting e-mail communications with patients. As a result, we decided to make the use of encryption in the transmission process an addressable implementation specification.
188037	Under the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act (HIPAA), is the billing for drugs by a Home Infusion Therapy provider considered a retail pharmacy drug claim transaction that would require billing the drugs and biologics using the National Council for Prescription Drug Programs (NCPDP) formats, and billing for other Home Infusion Therapy components, such as supplies and services, using the ASC X12N 837 format?	No. When a patient receives Home Infusion Therapy, the episode of Home Infusion Therapy typically has components of professional services and products that include ongoing clinical monitoring care coordination, supplies and equipment, and the drugs and biologics administered – all supplied by the Home Infusion Therapy provider. For this encounter, the drugs and biologics are billed on a claim for Home Infusion Therapy services as one of numerous components that comprises the claim. Although Home Infusion Therapy providers may be licensed as retail pharmacies in some states, their model for dispensing drugs and biologics for infusion, injection, or inhalation using a nebulizer, as well as dispensing total parenteral and enteral nutrition, is very different from that of traditional retail pharmacies. While the NCPDP claim format works well for the typical drug-dispensing activities performed by traditional retail pharmacies, it does not meet the administrative, clinical, coordination of care, and medical necessity requirements for Home Infusion Therapy claims. The ASC X12N 837 is the required standard format for claims for the provision of Home Infusion Therapy. Claims for Home Infusion Therapy care include the drugs, biologics, and nutrition components of the total Home Infusion Therapy encounter. Examples: 1-A licensed retail pharmacy's business is providing Home Infusion Therapy. Supplied by the pharmacy are professional services, products, and supplies and equipment, that include ongoing clinical monitoring and care coordination. Also supplied are the drugs and biologics administered by infusion, injection, or inhalation using a nebulizer, as well as total parenteral and enteral nutrition products and care. The ASC X12N 837 claim standard must be used for billing the drugs, biologics, parenteral nutrition and enteral nutrition that are provided by the pharmacy, and usually billed along with the service, supply, and equipment components of Home Infusion Therapy, i.e. comprising a total claim for Home Infusion Therapy.

		2-A licensed retail pharmacy has multiple lines of business, one of which is a traditional retail pharmacy, such as a walk-in community pharmacy, and a second of which is to provide Home Infusion Therapy as described in Example 1. The NCPDP claim standard must be used for billing drugs and biologics that are dispensed by the line of business performing the traditional single event filling of prescriptions, without also supplying the ongoing clinical monitoring and care coordination involved with an episode of Home Infusion Therapy. However, the ASC X12N 837 claim standard must be used for billing the drugs, biologics, parenteral nutrition and enteral nutrition that are provided by the pharmacy, and usually billed along with the service, supply, and equipment components of Home Infusion Therapy, i.e. comprising a total claim for Home Infusion Therapy. 3-A licensed retail pharmacy could dispense drugs used for home infusion therapy during its normal course of business dispensing traditional retail drug prescriptions, but the pharmacy does not provide the ongoing clinical monitoring and care coordination involved with an episode of Home Infusion Therapy. In this situation, the NCPDP claim format must be used for billing the home infusion therapy drugs. This is because a licensed retail pharmacy that happens to fill a prescription for a drug used in Home Infusion Therapy is not supplying the service components of the Home Infusion Therapy episode of care, and the NCPDP format is the adopted standard for retail pharmacy drug claims.
188138	I am a large pharmacy provider with Home Infusion Therapy and End Stage Renal Disease (ESRD) drugs and supplies (for home dialysis) business components. What HIPAA format is required for my home dialysis claims?	The drugs, products, and services provided by End Stage Renal Disease (ESRD) suppliers to home dialysis patients are considered Home Infusion Therapy for purposes of HIPAA-compliant claims transactions. When a patient receives Home Infusion Therapy, the episode of Home Infusion Therapy typically has components of professional services and products that include ongoing clinical monitoring, care coordination, supplies and equipment, and the drugs and biologics administered – all supplied by the Home Infusion Therapy provider. For this encounter, the drugs and biologics are billed on a claim for Home Infusion Therapy services, as one of numerous components that comprises the claim. The HIPAA standard format for claims for drugs, supplies, and services supplied by a Home Infusion Therapy provider is the ASC X12N 837 4010 as amended by 4010A1. The HIPAA standard claim format for drugs and biologics supplied by retail pharmacies is the National Council for Prescription Drug Programs (NCPDP) Standard Telecommunications Guide Version 5.1 and the NCPDP Batch Standard Batch Implementation Guide Version 1.1.
188739	When Can Covered Entities Disclose Information on Medicare Beneficiaries to QIOs?	Medicare Quality Improvement Organizations (QIOs) perform certain review and other functions for the Centers for Medicare & Medicaid Services (CMS) under contracts with CMS. These functions are required under Part B of Title XI of the Social Security Act. Part B of Title XI also requires that covered entities disclose information on Medicare beneficiaries to QIOs so that QIOs can perform the requirements under their Medicare contracts. Covered entities that conduct certain electronic transactions and are subject to the Privacy Rule of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) generally cannot disclose protected health information on Medicare beneficiaries or other patients without permission of the patients, unless the rule otherwise allows disclosure. If a covered entity's disclosure is required by law, the rule allows disclosure without the patient's permission under 45 CFR § 164.512(a). Therefore, when a covered entity discloses to a QIO information on Medicare beneficiaries that the QIO needs in order to perform under its contract with CMS, patient permission is not required.

1888 40	When Can Covered Entities Disclose Information on Non-Medicare Patients to QIOs?	Covered entities may also disclose protected health information about non-Medicare patients without their permission when the information involves the QIO's quality-related activities under its contract. Generally, when QIOs receive this information, they are functioning as health oversight agencies under §164.512(d). The HIPAA Privacy Rule defines a health oversight agency to include a Federal or other governmental agency or authority that is authorized by law to oversee the health care system (whether public or private), or government programs in which health information is necessary to determine eligibility or compliance with program standards (45 CFR § 164.501). Oversight agencies also include a person or entity acting under a contract with the public agency. Part B of Title XI requires Medicare QIOs, as CMS' contractors, to conduct activities necessary for appropriate oversight of the health care system. Specifically, Medicare QIOs *are health oversight agencies* to the extent that they are acting under contract with Medicare to oversee the health care system in general or compliance with quality standards under Medicare. This includes collecting and reviewing quality performance measures from hospitals regarding Medicare and non-Medicare patients, such as reports on surgical infection prevention, acute myocardial infarction and influenza and pneumococcal immunization. When a QIO is acting as a health oversight agency, disclosures to them for health care oversight purposes are permissible without patient permission.
1889 41	Are Covered Entities Protected When They Make Disclosures to QIOs?	The Social Security Act provides certain protections to those who disclose information to the QIOs, as described in §1157 of the Act. Under §1157, no person providing information to a QIO will be held, by reason of having provided such information, to have violated any criminal law or to be civilly liable under any State or Federal law, unless the information provided is unrelated to the performance of the contract of the QIO or the information is false and the individual knew or had reason to believe that the information was false.
1917 42	Is it necessary to have a business associate agreement between the provider and state or federal surveyors before a survey of the facility can be done?	Surveyed entities do not need to execute a business associate agreement with federal or state surveyors prior to releasing protected health information (PHI) as surveyors are "health oversight" agencies and not business associates of the surveyed entities under the HIPAA Privacy Rule definition of "business associate."
1918 43	Is it necessary for the provider to obtain the permission of the subject of protected health information (i.e., the patient) before a record is released to a health oversight agency for survey and certification work?	The HIPAA Privacy Rule provides that protected health information (PHI) may be used and disclosed without the authorization of the subject of that information for health oversight activities that are authorized by law. Examples are inspection, licensure and other activities necessary for the appropriate oversight of entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards. The HIPAA Privacy Rule also provides that PHI may be used and disclosed without the authorization of the subject of that information to the extent a law requires the production of that information.
1919 44	In the final Security Standards Rule published in the Federal Register on	If an implementation specification is described as "required", the specification must be implemented. The concept of "addressable implementation specifications" was developed to provide covered entities additional

	February 20, 2003, what is the difference between addressable and required specifications?	flexibility with respect to compliance with the security standards. In meeting standards that contain addressable implementation specifications, a covered entity will do one of the following for each addressable specification: (a) implement or the addressable implementation specifications; (b) implement one or more alternative security measures to accomplish the same purpose; (c) not implement either an addressable implementation specification or an alternative. The covered entity must decide whether a given addressable implementation specification is a reasonable and appropriate security measure to apply within its particular security framework. This decision will depend on a variety of factors, such as, among others, the entity's risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation. The decisions that a covered entity makes regarding addressable specifications must be documented.
1987 45	Is a flexible spending account or a cafeteria plan a covered entity for purposes of the Privacy Rule and the other HIPAA, Title II, Administrative Simplification standards?	A "group health plan" is a covered entity under the Privacy Rule and the other HIPAA, Title II, Administrative Simplification standards. A "group health plan" is defined as an "employee welfare benefit plan," as that term is defined by the Employee Retirement Income Security Act (ERISA), to the extent that the plan provides medical care. See 42 USC § 1320d(5)(A) and 45 CFR 160.103. Thus, to the extent that a flexible spending account or a cafeteria plan meets the definition of an employee welfare benefit plan under ERISA and pays for medical care, it is a group health plan, unless it has fewer than 50 participants and is self-administered. Employee welfare benefit plans with fewer than 50 participants and that are self-administered are not group health plans. Flexible spending accounts and cafeteria plans are not excluded from the definition of "health plan" as excepted benefits. See 45 CFR 160.103, paragraph (2)(i) of the definition of "health plan."
2006 46	When would a billing service be considered a health care clearinghouse?	Many health care providers outsource their claims management functions to billing services. Billing services may provide a wide range of back office services to health care providers including coding, data entry, charge entry, insurance claims submissions, posting receipts, filing secondary insurance claims, balance billing for coinsurance and deductibles, managing accounts receivables, and other practice management services. Sometimes, a billing service may convert a paper claim, received from a health care provider, to an electronic claim, and submit the electronic claim to a health plan as an electronic transaction. In such cases, a billing service may need to aggregate information necessary for claim submission from various sources such as charge slips, paper bills, medical records, etc. and/or from various entities prior to generating an electronic claim. In addition, billing services may also convert electronic claims in provider proprietary formats, obtained from one file/batch or several separate files or batches, into a HIPAA-compliant standard transaction format, or visa versa, prior to transmitting to a health plan or a health care provider. The HIPAA regulations at 45 CFR §160.103 define a health care clearinghouse. An entity that meets the definition of health care clearinghouse is a covered entity under HIPAA. The term “health care clearinghouse” is defined as a public or private entity…that does either of the following functions: (1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction. (2) Receives a standard transaction from another entity and processes or facilitates the processing of health

information into nonstandard format or nonstandard data content for the receiving entity.

Given that the designation of an entity as a health care clearinghouse requires an examination of the functions of the entity, questions have arisen as to when a billing service's functions or activities make the billing service a health care clearinghouse such that it is a covered entity for purposes of HIPAA.

In some cases, the business relationships that exist among health care providers, billing services, health care clearinghouses, and health plans affect their relative statuses as covered entities. The following examples of contractual arrangements between health care providers, billing services, health care clearinghouses, and health plans illustrate when and how such arrangements confer HIPAA covered entity status on a billing service.

1. Billing Service 1 is a Health Care Clearinghouse. A health care provider sends claims data on paper to Billing Service 1, with which it has a contractual arrangement whereby Billing Service 1 converts the paper data into the standard claim transaction and then transmits it to a health plan. Billing Service 1 is a health care clearinghouse because it receives non-standard data and converts it into a standard transaction.

   Conversely, a health care provider has a contractual arrangement with Billing Service 1 whereby Billing Service 1 converts standard electronic remittance advices into non-standard format for transmission to the health care provider. Billing Service 1 is a health care clearinghouse because it receives standard transactions and converts them into non-standard format.

2. Billing Service 2 is a Health Care Clearinghouse. A health care provider sends claims data on paper to Billing Service 2, with which it has a contractual arrangement whereby Billing Service 2 converts the paper data into the standard claim and transmits it to a health plan. Billing Service 2, in order to fulfill that contractual arrangement, has an agreement with Health Care Clearinghouse A whereby Health Care Clearinghouse A receives the paper data from Billing Service 2, converts it into the standard claim, and transmits it to a health plan. Essentially, Billing Service 2 has out-sourced the translation function to Health Care Clearinghouse A. Because Billing Service 2 has contracted with the provider to perform clearinghouse functions (which it does by outsourcing the clearinghouse function to Health Care Clearinghouse A), Billing Service 2 is a health care clearinghouse.

3. Billing Service 3 is NOT a Health Care Clearinghouse. A health care provider has a contractual arrangement with Billing Service 3 whereby Billing Service 3 conducts various claims preparation services and then transmits non-standard claims to Health Care Clearinghouse B for conversion into standard format and transmission to the health plan. The health care provider has a contractual arrangement with Health Care Clearinghouse B whereby Health Care Clearinghouse B receives the non-standard claims from Billing Service 3, converts the data to standard, and transmits it to a health plan. Billing Service 3 is NOT a health care clearinghouse because it neither converts non-standard (paper or electronic) data into the standard claim transaction, nor does it out-source this function.

4. Billing Service 4 is NOT a Health Care Clearinghouse. A health care provider sends claims data on paper to Billing Service 4, with which it has a contractual arrangement whereby Billing Service 4 conducts various claims preparation services and then transmits a paper claim to a health plan or to Health Care

		Clearinghouse C. The health plan has a business associate agreement with Health Care Clearinghouse C whereby Health Care Clearinghouse C converts the paper claim to standard claim format and then transmits the standard claim to the health plan. Either the health plan itself, or Health Care Clearinghouse C, converts the paper claim from non-standard format into a standard claim. Billing Service 4 is NOT a health care clearinghouse because it neither converts non-standard data into a standard, nor does it out-source this function.
2007 47	Does a health care clearinghouse have a business associate arrangement with the entity it serves?	An entity that receives paper and/or electronic health data from a single source or from multiple sources, and converts that data from non-standard formats or data elements into a HIPAA standard transaction is a health care clearinghouse. The health care clearinghouse may be acting on behalf of either a health care provider or a health plan and, therefore, may have a business associate relationship with either the health care provider or the health plan. Conversely, an entity that receives a HIPAA standard transaction and converts that transaction into non-standard format or data elements (paper and/or electronic) is also a health care clearinghouse. Again, the health care clearinghouse may have a business associate relationship with either a health care provider or a health plan. Whether a health care clearinghouse is a business associate in either of the two situations above will depend on the status of the entity on whose behalf it is acting. If the health care clearinghouse is acting on behalf of a health care provider or an insurer that is not a covered entity under HIPAA, the health care clearinghouse would not be a business associate as defined in HIPAA regulations at 45 CFR §160.103. The following examples are the same factual scenarios as those addressed in our answer to the question "When would a billing service be considered a health care clearinghouse?" These examples address the covered entity status of the health care providers in the examples rather than the billing services (the latter is addressed in our answer to the question "When would a billing service be considered a health care clearinghouse?). ▪ Billing Service 1 is a Business Associate. A health care provider sends claims data on paper to Billing Service 1, with which it has a contractual arrangement whereby Billing Service 1 converts the paper data into the standard claim transaction and then transmits it to a health plan. The health care provider is a covered entity because it is, through Billing Service 1, transmitting a standard claim transaction to a health plan. Because Billing Service 1 is acting on behalf of a covered entity (and performing functions referred to in 45 CFR § 160.103, definition of "Business associate"), Billing Service 1 is a business associate. ▪ Billing Service 2 is a Business Associate. A health care provider sends claims data on paper to Billing Service 2, with which it has a contractual arrangement whereby Billing Service 2 converts the paper data into the standard claim and transmits it to a health plan. Billing Service 2, in order to fulfill that contractual arrangement, has an agreement with Health Care Clearinghouse A whereby Health Care Clearinghouse A receives the paper data from Billing Service 2, converts it into the standard claim, and transmits it to a health plan. The health care provider is a covered entity because it is, through Billing Service 2, transmitting a standard claim transaction to a health plan. Because Billing Service 2 is acting on behalf of a covered entity (and performing functions referred to in 45 CFR § 160.103, definition of "Business associate"), Billing Service 2 is a business associate. ▪ Billing Service 3 is a Business Associate. A health care provider has a contractual arrangement with

		Billing Service 3 whereby Billing Service 3 conducts various claims preparation services and then transmits non-standard claims to Health Care Clearinghouse B for conversion into standard format and transmission to the health plan. The health care provider has a contractual arrangement with Health Care Clearinghouse B whereby Health Care Clearinghouse B receives the non-standard claims from Billing Service 3, converts the data to standard, and transmits the standard claim to a health plan. The health care provider is a covered entity because it is, through Health Care Clearinghouse B, transmitting a standard claim transaction to a health plan. Because Billing Service 3 is acting on behalf of a covered entity (and performing functions referred to in 45 CFR § 160.103, definition of "Business associate"), Billing Service 3 is a business associate. ▪ Billing Service 4 is NOT a Business Associate. A health care provider sends claims data on paper to Billing Service 4, with which it has a contractual arrangement whereby Billing Service 4 conducts various claims preparation services and then transmits a paper claim to a health plan or to Health Care Clearinghouse C. The health plan has a business associate agreement with Health Care Clearinghouse C whereby Health Care Clearinghouse C converts the paper claim to standard claim format and then transmits the standard claim to the health plan. Either the health plan itself, or Health Care Clearinghouse C, converts the paper claim from non-standard format into a standard claim transaction. The health care provider is NOT a covered entity (assuming that the health care provider does not conduct any other standard transactions electronically), because it is not transmitting an electronic claim to a health plan, nor is Billing Service 4 transmitting an electronic claim to a health plan on behalf of the health care provider. The fact that the health plan or Health Care Clearinghouse C converts paper claims data into a standard transaction does not make the health care provider a covered entity. Because Billing Service 4 is acting on behalf of an entity that is not a covered entity, Billing Service 4 is NOT a business associate.
200848	Can a billing service be a business associate of a covered entity and not be a health care clearinghouse?	Yes. Example: Billing Service 3 is a Business Associate but is NOT a Health Care Clearinghouse. A health care provider has a contractual arrangement with Billing Service 3 whereby Billing Service 3 conducts various claims preparation services and then transmits non-standard claims to Health Care Clearinghouse B for conversion into standard format and transmission to the health plan. The health care provider has a contractual arrangement with Health Care Clearinghouse B whereby Health Care Clearinghouse B receives the non-standard claims from Billing Service 3, converts the data to standard, and transmits the standard claim to a health plan. The health care provider is a covered entity because it is, through Health Care Clearinghouse B, transmitting a standard claim transaction to a health plan. Because Billing Service 3 is performing claims preparation services on behalf of a covered entity, Billing Service 3 is a business associate. Billing Service 3 is not a health care clearinghouse because it neither converts non-standard (paper or electronic) data into the standard claim transaction, nor does it out-source this function
232049	What is an acceptable contingency plan?	An acceptable contingency plan is whatever is appropriate for the individual plan's situation in order to ensure the smooth flow of payments. Health plans will need to make their own determinations regarding contingency plans based on their unique business environments. A contingency plan could include, for example,

		maintaining legacy systems, flexibility on data content or interim payments. Other more specific contingency plans may also be appropriate. For example, a plan may decide to continue to receive and process claims for supplies related to drugs using the NCPDP format rather than the 837 format currently specified in the regulations. The appropriateness of a particular contingency or the basis for deploying the contingency will not be subject to review.
232150	Is it acceptable for a health plan to announce its contingency now?	Yes. Health plans should announce their contingency plans as soon as possible to allow their trading partners enough time to make any needed adaptations to their business operations to ensure minimal disruptions. In deciding whether to deploy a contingency plan, organizations would have to make an assessment of their outreach and testing efforts to assure they made a "good faith" effort.
232251	How does a covered entity demonstrate good faith?	Covered entities should keep track of the efforts they have made – both before and after the October 16 compliance date – to become compliant. For a provider, that could include your efforts to work with vendors, clearinghouses and submitters to schedule testing with plans, and the results of those tests. For a plan, it could include keeping track of outreach activities (letters, conferences, phone calls, etc.) encouraging providers/submitters to schedule testing, testing schedules, and statistics showing increased testing results.
232352	Will Medicare be ready on October 16, 2003?	Yes. Medicare already accepts HIPAA-compliant transactions.
232453	Who will determine whether I made a good faith effort?	The Office of HIPAA Standards within the Centers for Medicare & Medicaid Services (CMS) is responsible for enforcing the electronic transactions and code sets provisions of the law. When OHS receives a complaint about a covered entity, it would ask the entity to demonstrate their reasonable and diligent efforts to become compliant and, in the case of health plans, to facilitate the compliance of their trading partners. Strong emphasis will be placed on sustained actions and demonstrable progress in determining a covered entity's good faith effort.
232754	What kind of activities is Medicare doing to demonstrate good faith efforts?	CMS has directed the Medicare contractors to intensify all HIPAA outreach and testing efforts with their respective provider and submitter communities and trading partners. Contractors are communicating HIPAA information via individual provider contacts, published provider bulletins, websites, and many other mechanisms. CMS also provides HIPAA information via web casts, videos, advertising in industry publications, and audio conferences.
232855	Has Medicare announced its contingency plan?	Yes. On September 23, 2003 CMS announced that it will implement a contingency plan for the Medicare program to accept noncompliant electronic transactions after the October 16, 2003 compliance deadline. This plan will ensure continued processing of claims from thousands of providers who will not be able to meet the deadline and otherwise would have had their Medicare claims rejected. CMS made the decision to implement its contingency plan after reviewing statistics showing unacceptably low numbers of compliant claims being submitted. The contingency plan permits CMS to continue to accept and process claims in the electronic formats now in use, giving providers additional time to complete the testing process. CMS will regularly reassess the readiness

		of its trading partners to determine how long the contingency plan will remain in effect.
232956	Can mental health practitioners, agencies, institutions and others still use DSM-IV diagnostic criteria, even though DSM-IV has not been adopted as a HIPAA code set?	Yes. Adoption of the diagnostic criteria, which are used to establish a diagnosis, is outside the scope of HIPAA. Congress enacted HIPAA for the purpose of standardizing the form and content of certain electronic transactions, and not for the purpose of standardizing the diagnostic criteria applied by clinicians. The basic purpose for adopting code sets under HIPAA is to standardize the "data elements" used in the electronic processing of certain administrative and financial health care transactions. While the patient's diagnosis is a data element used in such transactions, the criteria considered by the clinician in reaching a diagnosis are not. Practitioners are free to use the DSM-IV diagnostic criteria—or any other diagnostic guidelines—without any HIPAA-related concerns.
233057	The ICD-9-CM includes a glossary with definitions for mental disorders found in Appendix B. Are clinicians required to use these glossary definitions when using the ICD-9-CM codes?	No. HIPAA does not require clinicians to adhere to the glossary definitions in Appendix B. The ICD-9-CM itself does not require clinicians to adhere to the glossary definitions. With respect to these definitions, the Introduction to the ICD-9-CM states only that Appendix B has been "included as a reference to the user to further define a diagnostic statement." This statement suggests that the glossary definitions are advisory only, and not mandatory. While HHS has adopted the ICD-9-CM as a HIPAA code set for diagnosis, it has not mandated the use of the glossary definitions.
233158	In current practice by the mental health field, many clinicians use the DSM-IV in diagnosing mental disorders. Can these clinicians continue current practice and use the DSM-IV diagnostic criteria?	Yes. The Introduction to the DSM-IV indicates that the DSM-IV is "fully compatible" with the ICD-9-CM. The reason for this compatibility is that each diagnosis listed in the DSM-IV is "crosswalked" to the appropriate ICD-9-CM code. It is expected that clinicians may continue to base their diagnostic decisions on the DSM-IV criteria, and, if so, to crosswalk those decisions to the appropriate ICD-9-CM codes. In addition, it is still perfectly permissible for providers and others to use the DSM-IV codes, descriptors and diagnostic criteria for other purposes, including medical records, quality assessment, medical review, consultation and patient communications.
234859	Must a health plan reject an entire batch of standard transactions if one or more of those transactions are HIPAA-compliant?	No. Neither the law nor our regulations require a health plan to reject an entire batch of standard transactions if one or more of those transactions are HIPAA-compliant. Health plans are allowed to accept and process any and all claims within a batch that meet the HIPAA requirements
234960	What are Companion Guides? Where do I get them?	Companion Guides are health plan-specific versions of the HIPAA-adopted standard Implementation Guides that define the health plans' requirements for situational data elements, and provide special instructions and further guidance on how the health plan is interpreting the HIPAA Implementation Guides. While HIPAA adopted specific Implementation Guides, Companion Guides have been independently created by some health plans to supplement the HIPAA Implementation Guides and are tailored to meet individual health plans' particular needs. Companion Guides are not required by HIPAA, and all health plans are not publishing Companion Guides. These guides cannot: 1-Change the definition, data condition, or use of a data element or segment in a standard.

		2-Add any data elements or segments to the maximum defined data set. 3-Use any code or data elements that are either marked "not used" in the standard's implementation specification or are not in the standard's implementation specification(s). 4-Change the meaning or intent of the standard's implementation specification(s). Companion Guides may be requested from specific health plans that have published them.
235061	Are credit card transactions covered under HIPAA? If an individual (i.e., a subscriber or a patient) uses his or her credit or debit card to pay for premiums, deductibles and/or co-payments, is that "transaction" considered a HIPAA standard, and must it be in a HIPAA compliant format with HIPAA compliant content?	The HIPAA standards must be used by "covered entities," which are health plans, health care clearinghouses and health care providers who conduct any of the standard transactions electronically. The HIPAA standards do not apply to individuals, unless they are acting in some capacity on behalf of a covered entity, and not on behalf of themselves as, for example, subscribers or patients. An individual, acting on behalf of himself or herself, is not a covered entity, and is therefore not subject to the HIPAA standards. Transactions conducted between subscribers or patients and health plans or health care providers are not transactions for which the Secretary of Health and Human Services has adopted standards. Therefore, if an individual uses a personal credit card or debit card to pay either a premium, co-payment and/or deductible to a health plan or a health care provider, the individuals are not covered entities, they are not conducting covered transactions, and the transactions being conducted need not be in the standard format.
235162	The Transactions Final Rule requires that medical data codes that are valid at the time health care is furnished be used for reporting services. When reporting inpatient hospital or other extended stay facility services that span a range of dates, what date do I use as the date of service to determine valid medical codes?	For inpatient claims use the date of discharge as the date to determine valid medical codes, and other codes that are dependent upon service date for validity. For outpatient claims, the actual date that the service is rendered is reported with the service item at the line level, and used to determine valid medical codes and other codes that are subject to service date for validity.
235263	Is the transaction created by the use of a debit or credit card for a Flexible Spending Account (FSA) or a Health Reimbursement Account (HRA) subject to the adopted standard transactions required	A beneficiary's use of an FSA's or HRA's debit or credit card for payment of out-of-pocket expenses at a pharmacy or provider's office, that routinely accepts traditional credit card payments, is comparable to any payment to a health care provider using a conventional credit card. Debit and credit card transmissions for these transactions are not subject to the HIPAA EDI requirements, and are considered transactions between the beneficiary and a provider, not a health plan and a provider.

	by HIPAA?	
235364	Where can I get help locating and interpreting the Implementation Guides for the standard transactions?	The Implementation Guides for the Accredited Standards Committee (ASC) X12N transactions are available for free, from the Washington Publishing Company, at www.wpc-edi.com. You will need to create a log in and ID code but there is no charge for this set up. The Implementation Guides for the NCPDP retail pharmacy transactions are available from the National Council for Prescription Drug Programs at www.ncpdp.org. If you have questions about the Implementation Guides, you can attempt to work through the issues with your software vendor, health care clearinghouse or the EDI contact at your trading partner organizations. For very technical questions, you should contact either X12N or NCPDP, as appropriate, at www.x12.org or www.ncpdp.org, respectively.
235465	Does HIPAA allows you to network computers? In other words, are covered entities allowed to connect two computer systems, either within the covered entity, or between two covered entities or between a covered entity and its business associate(s) so that they can exchange information directly?	With regard to networking computers, there is nothing in the HIPAA Security Rule that prohibits the networking of computers, whether inside the same company, or between two unrelated companies who conduct business together. However, the covered entity must demonstrate that it has evaluated the risks associated with a network connection, and document that it has established all of the safeguards (technical, physical and administrative) that would serve to protect the information that is exchanged along the network. That will include an assessment of everything from the firewall to the designation and training of the individuals who have access to the data.
235566	What can providers do when they cannot obtain the Social Security number (SSN) or Employer Identifier number (EIN) of physicians in order to prepare HIPAA-compliant claims? Must this information be reported on standard transactions if the provider submitting the claim or encounter information transaction does not have the information because the physician refuses to disclose it?	The X12N Implementation Guides require the SSN, the EIN, or the National Provider Identifier (NPI) to be reported in NM109 (Identification Code) for the certain physicians under certain situations in the claim or encounter information transaction. (When the NPI is implemented, the NPI will be the required, and the only allowable, entry for NM109.) For example, if the Rendering Provider is not also the Billing Provider, the Primary Identifier is required for the Rendering Provider The expectation, at the time the Implementation Guides were written, was that the NPI would be implemented before the compliance date for the Transactions and Code Sets standards, which is October 16, 2003. That will not be the case. Therefore, either the SSN or the EIN must be reported in NM109, as described above, beginning October 16, 2003. This requirement is causing problems for certain providers who must report, but do not have, that information. This requirement places a burden on providers that report services of, or referrals by, providers for whom they do not have SSNs or EINs because they must obtain the SSN or the EIN from those providers in order to report that information on claims. We are aware that some providers are reluctant, or even refuse, to furnish that

		information when requested to do so for this purpose. The refusal to furnish SSNs or EINs to providers that are attempting to submit HIPAA-compliant claims impedes the business of health care. Claims without required data may very well be rejected or the services denied by health plans. Rejections and denials will eventually affect the cash flow to the providers attempting to submit HIPAA-compliant claims and, in the end, may affect the availability of health care to patients. It is imperative that providers disclose their SSNs or EINs to providers that request that information in order to create HIPAA-compliant claims.
235667	What are the Healthcare Provider Taxonomy codes? Where may I obtain a copy of the codes?	The Healthcare Provider Taxonomy codes are a HIPAA standard code set named in the implementation specifications for some of the ASC X12N standard HIPAA transactions. The "Healthcare Provider Taxonomy Code" is a situational data element in the X12N Implementation Guides for the 837 4010A1 Institutional and Professional claims/encounter information transactions. If the Taxonomy code is required in order to properly pay or process a claim/encounter information transaction, it is required to be reported. Thus, reporting of the Healthcare Provider Taxonomy Code varies from one health plan to another. The Healthcare Provider Taxonomy code set divides health care providers into hierarchical groupings by type, classification, and specialization, and assigns a code to each grouping. The Taxonomy consists of two parts: individuals (e.g., physicians) and non-individuals (e.g., ambulatory health care facilities). All codes are alphanumeric and are 10 positions in length. These codes are not "assigned" to health care providers; rather, health care providers select the taxonomy code(s) that most closely represents their education, license, or certification. If a health care provider has more than one taxonomy code associated with it, a health plan may prefer that the health care provider use one over another when submitting claims for certain services. The Healthcare Provider Taxonomy code set is available at no charge from the Washington Publishing Company's website: www.wpc-edi.com. The Healthcare Provider Taxonomy code set is maintained by the National Uniform Claim Committee (NUCC). The NUCC accepts requests for new codes and requests for changes to existing codes or descriptions. The criteria for review of a request for a new code or a change are available on the NUCC web site (www.nucc.org). The code set is updated twice a year.
235768	Can ICD-9-CM procedure codes be reported on hospital outpatient claims? If I use HCPCS codes to report hospital outpatient services at the "required" service line level segment for a claim, may I use the ICD-9-CM procedure codes to report hospital outpatient services at	NO. ICD-9-CM procedure codes were named as the HIPAA standard code set for inpatient hospital procedures. The ICD-9-CM procedure codes were not named a HIPAA standard for procedures in other settings such as hospital outpatient services or other types of ambulatory services. Hospitals may capture the ICD-9-CM procedure codes for internally tracking or monitoring hospital outpatient services; but when conducting standard transactions, hospitals must use HCPCS codes to report outpatient services at the service line level and the claim level, if the situation applies. Even though an ICD-9-CM procedure code qualifier is available, in addition to a HCPCS code qualifier, at the "situational" claim level segment, the Transactions and Code Sets regulation states that ICD-9-CM procedure codes is the adopted standard code set for hospital inpatient services.

	the claim level "situational" segment?	In order to continue operations and maintain cash flow, providers, as part of their contingency plan, could continue to report hospital outpatient services with ICD-9-CM procedure codes if required by the health plan. However, health plans must realize that reporting hospital outpatient services with ICD-9-CM procedures codes on standard claim transactions is not compliant, and that their good faith efforts to come into compliance must include the steps being taken to change this requirement.
235869	Is the use of local codes permitted after October 15, 2003?	Covered entities are required to conduct covered transactions in standard form as of October 16, 2003 if they received a one-year extension of the original effective date specified in the HIPAA Transactions Rule, published August 17, 2000. All States requested and received such extensions. Covered entities must use standard code sets (and, therefore, may not use local procedure codes and modifiers) in conducting covered transactions. Section 532 of the Medicare, Medicaid, and State Child Health Insurance Program (SCHIP) Benefits Improvement and Protection Act of 2000 (BIPA) allows an exception to the effective date specified in the HIPAA Transactions Final Rule, by authorizing the Secretary to allow public use of HCPCS Level III codes through December 31, 2003. The BIPA defines "HCPCS Level III codes" as "the alphanumeric codes for local use under the Health Care Financing Administration [now Healthcare] Common Procedure Coding System (HCPCS)". HCPCS codes are used to report certain procedures, services, and supplies. Only Medicare, Medicaid State agencies, and SCHIP programs (where applicable) that use HCPCS Level III codes and modifiers may continue their use to report medical procedures, services, or supplies through December 31, 2003. Also Medicare and Medicaid MCOs may continue to use Medicare/Medicaid related HCPCS Level III codes and modifiers for Medicare/Medicaid business with dates of service through December 31, 2003. Procedure codes describe services, durable medical equipment, prosthetics, orthotics, supplies, and drugs. Modifiers are used to indicate that a service or procedure that has been performed has been altered by some specific circumstance, but not changed in its definition or code. CMS considers HCPCS Level III codes, as used in this BIPA provision, to apply to both the HCPCS Level III procedure codes and modifiers that Medicare had approved for local Medicare carrier and fiscal intermediary use and to the local procedure codes and modifiers that State Medicaid agencies and SCHIP programs had developed and used for their own purposes. Therefore, local procedure codes and modifiers developed by State Medicaid and SCHIP programs, as well as the Medicare-approved local procedure codes and modifiers may be used for procedures with dates of service through December 31, 2003. While this interpretation provides additional time for Medicare, individual State Medicaid agencies, SCHIP programs, and Medicare and Medicaid MCOs to come into compliance with certain HIPAA standards, these entities are not required to continue to use HCPCS Level III codes and modifiers for procedures with dates of service beyond October 15, 2003. This extension does not apply to local codes and modifiers that are not HCPCS Level III codes and were developed for reporting information other than procedures, including but not limited to gender, provider taxonomy/specialty, and diagnosis.
2398	What code should be used in	At the time the X12N Implementation Guides were adopted, neither the Privacy Rule nor the Modifications to

70	data element "Release of Information Code," which is captured in data elements CLM09 and O106 of the X12N 837 Institutional and Professional Claims, version 4010A1? The code indicates whether the provider has on file a signed statement by the patient authorizing the release of medical data to other organizations. Doesn't the Privacy Rule obviate the need for a patient to sign such a statement?	the Privacy Rule had been published. Several States, though, had and still have patient confidentiality laws that require the patient's consent to disclose certain health information. Those State laws that are more stringent than the Privacy Rule requirements remain valid and enforceable; they are not preempted by the Privacy Rule. Similarly, certain federal laws and regulations require in many circumstances a patient's consent for disclosing health information regarding alcohol and drug abuse prevention and treatment services. If one of those State or federal laws applies, any one of the codes for the CLM09 or O106 data elements could apply. X12N, the developer of the subject Implementation Guides, is aware of the impact of the Privacy Rule, which under limited circumstances permits the use and disclosure of certain health information without the patient's consent. More specifically, a covered entity is not required by 45 CFR 164.502 to obtain a patient signature in order to release claim-related information for routine health care delivery services (known as treatment, payment, and health care operations). In those cases in which the Privacy Rule applies and a more stringent State law or another federal law does not apply, HHS and X12N would consider "Release of Information Codes" I (Informed consent to release medical information for conditions or diagnoses regulated by Federal statutes) or Y (Yes, provider has a signed statement permitting release of medical billing data related to a claim) to be valid and the most appropriate for use. It is also important to note that HHS and X12N interpret the scope of these data elements to be limited to authorizing the release of information contained within the specific claim at hand.
2431 71	Can only Medicare's DRG codes be used on standard transactions? The X12N Implementation Guides indicate that the source of the Diagnosis Related Group (DRG) code set is "Source 229, Federal Register or HIM-15." Source 229 is defined as HCFA (now CMS). "Federal Register" is vague in that it could represent anything that CMS publishes in the Federal Register. HIM-15 is the Medicare Provider Reimbursement Manual. Does this mean that only Medicare's DRG codes can be used on standard	There are several DRG code sets in addition to the Medicare DRG code set that are currently used within the healthcare industry. CMS, which maintains HIM-15, has added language to Part 1, Chapter 28, section 2801 of HIM-15 that permits the use of DRG codes other than Medicare DRG codes to be used on standard transactions.

	transactions?	
243972	Does HIPAA permit the use of V codes? Is their use consistent with OASIS requirements?	Yes. HIPAA standard transactions accept valid ICD-9 diagnosis codes, including V-codes, consistent with the HIPAA required use of the ICD-9 code set. HIPAA Administrative Simplification requirements only apply to specific electronic transactions including claims transmission. At this time OASIS is not one of the standard transactions adopted by HIPAA. However Medicare (not HIPAA) requires diagnostic coding to be consistent between OASIS supporting a home health episode, and a claim. Therefore, OASIS expanded its use of the ICD-9 diagnosis codes to permit the use of V-codes.
245673	Do the HIPAA transactions and code sets standards apply to paper claims and other non-electronic transactions?	NO. The HIPAA transactions and code sets standards only apply to electronic transactions conducted by covered entities. Other entities, such as employers or casualty insurance plans, may decide to use them voluntarily but are not required to do so. For paper transactions, health plans are free to set their own data requirements. Other federal or state laws may require plans or providers to use specific code sets for certain paper transactions. All covered health plans and providers must, however, be able to use the HIPAA standards for electronic transactions. Health plans may choose to require that paper claims include the same data elements, codes and identifiers, that are required by the HIPAA regulations for electronic transactions.
245774	Has HHS approved any pilot studies for new code sets to be used with the HIPAA standard transactions?	In accordance with the HIPAA regulations, in January 2003, the Secretary of HHS approved a pilot study for the use of Advanced Billing Concepts (ABC codes) to represent services for Alternative Medicine, Nursing and other Integrative Health Care. Interested participants were required to register with Alternative Link by May 29, 2003 in order to use the ABC codes in HIPAA standard transactions as of October 16, 2003.
245875	May I use Alternative Billing Concept codes (ABC codes) for HIPAA standard transactions even though they are not on the list of approved code sets?	In January 2003, the Secretary of HHS approved a pilot study for the use of Advanced Billing Concepts (ABC codes) for Alternative Medicine, Nursing and other Integrative Health Care. Covered entities interested in participating in the pilot, registered with Alternative Link by May 29, 2003. These registered participants and certain trading partners of those organizations may use ABC code sets for HIPAA transactions.
245976	Is a health care claim appeal considered a HIPAA-adopted standard transaction?	No, an appeal of a health care claim is not the same as a health care claim and does not qualify as a HIPAA standard transaction. The HIPAA regulations do not define the terms "*health care claim*" or "*claim appeal*." However, the regulations define a *health care claim or encounter transaction* as the transmission of either a) a request to obtain payment, along with the information required to support the request or b) a report of health care information to permit payment on a basis other than a direct claim. In contrast, a claim appeal is an action taken on a claim that has already been submitted. A claim submitter may appeal either a refusal to pay a claim, or the amount that was paid. HHS has not adopted an electronic transaction standard for the submission of claim appeals. Each health plan is free to establish its own requirements for appeals. If a plan requires a provider to re-submit a claim as part of its appeals process, that

		re-submission would qualify as a claim and should be submitted using the standard format. For Medicare claims only, the term "*initial Medicare claim*" is defined as a claim submitted to Medicare for payment under Part A or Part B of the Medicare program "for the first time for processing, including claims sent to Medicare for the first time for secondary payment purposes. *Initial Medicare claim* excludes any adjustment or appeal of a previously submitted claim, and claims submitted under Part C of the Medicare program...."
248077	Must a multi-functional single covered entity (e.g., functions as both a health plan and a provider) use a standard transaction when electronically transmitting standard transactions within the same covered entity?	Yes. A covered entity with multiple covered organizations under its umbrella (e.g., a health plan and a provider group), must use the standard (HIPAA) transactions when those organizations conduct any of the transactions internally. If the HIPAA regulation requires the use of the standard transaction for the specific transaction in question, then HIPAA rules apply. A transaction means the exchange of information between two parties to carry out financial or administrative activities. For example, a claims transaction is the exchange of information between a health care provider and health plan about services provided to a patient. The purpose of the transaction is for the provider to obtain payment. Similarly, an eligibility transaction is a request for information (from a provider or another health plan) to a health plan about a patients benefits and eligibility. If a health plan owns a provider group, the exchange of claim and payment information is not affected by the ownership arrangement; the requirement to exchange the transactions using HIPAA standards is based on the purpose of the transaction (i.e. to secure payment for the provider). "To determine if the exchange is a transaction, refer to the TCS final rule. The definition, purpose and use of each transaction is detailed in the regulations at Subpart K through R, Sections 162.1101 through 162.1801, and in the adopted Implementation Guides."
248178	If a health plan registered to participate in the Advanced Billing Concepts code set (ABC code) demonstration project, contracts with another insurance company to perform claims processing or administrative services on its behalf, may that second insurance company use the ABC codes to process those claims even if it did not register?	Yes. As long as the second insurance company acting as administrator is performing functions under the contract with the registered health plan, the contracted insurance company can use the Advanced Billing Concepts code set (ABC codes) for the processing of claims.
248279	Would a Preferred Provider Organization's (PPO)	Yes. The practitioners providing services under contract to the PPO would be covered by virtue of that

	registration in the (Advanced Billing Concepts (ABC) code set demonstration also cover the practitioners that it contracts with to provide services?	contractual relationship and would be permitted to use the ABC code set for their PPO patients.
251280	May a health plan require a provider to accept payment for a claim transaction via electronic fund transfer (EFT) as a condition for using the 835 remittance advice?	No. A provider has the right to request an 835 remittance advice from the health plan and the plan must comply. The plan may not require that the provider accept an EFT as a condition of using the 835. Section 162.925(a)(1) specifically addresses this point and states that, "if an entity requests a health plan to conduct a transaction as a standard transaction, the health plan must do so". Further, section 162.925(a)(2) states that "a health plan may not delay or reject a transaction or attempt to adversely affect the other entity or the transaction, because the transaction is a standard transaction". A business decision to only pay via EFT and to require providers to accept EFT versus paper checks should be negotiated and executed independent of the HIPAA transactions.
261081	What is the Office of HIPAA Standards?	The Department of Health and Human Services (DHHS), specifically the Office of HIPAA Standards (OHS) is responsible for HIPAA transactions and code sets (TCS) enforcement. OHS is an office within the Centers for Medicare & Medicaid Services (CMS), but for purposes of HIPAA enforcement, OHS operates independently and is completely detached from CMS's Medicare and Medicaid related activities.
261182	When should I file a HIPAA transaction and code set complaint with the federal government?	Filing a HIPAA transaction complaint with the federal government should be the last resort in efforts to resolve disputes. Parties should attempt to resolve technical issues and disputes on specific transactions and code set issues prior to filing a complaint. Trading partners should work together to resolve issues; and patients (or representatives of patients), should first try to resolve the issue with the provider and payer prior to registering a complaint. Various resources are available to the public to provide clarification on issues. The official HIPAA Implementation Guides, which can be downloaded at no cost at the Washington Publishing Company website at http://www.wpc-edi.com. Answers to technical questions are available from the organizations responsible for developing the standards. For assistance with the ANSI X12 transactions, go to the X12 website (www.X12.org). For technical assistance with the National Drug Codes standards, go to the NCPDP website (www.ncpdp.org). If all of these approaches have failed to resolve the HIPAA transaction dispute, file a complaint with the Office of HIPAA Standards (OHS) either electronically or by mail.
261283	Who can file a HIPAA transaction and/or code set complaint?	Anyone may file a valid complaint. The individual filing the complaint must be able to provide the details of the complaint, including all information necessary for OHS to resolve the complaint. Examples of unresolved transaction disputes might include: • The complainant received a non-compliant HIPAA file from a covered entity. • The complainant sent a compliant data file to a covered entity but they are rejecting it.

		• A covered entity that the complainant sends or receives data from has specified a non-compliant companion guide. For example, a companion guide must not specify additional fields beyond those specified by HIPAA. • Any other type of complaint against a covered entity that the complainant sends and receives HIPAA data
261384	How do I file a HIPAA complaint?	A HIPAA electronic transaction and/or code set complaint are filed to the Office of HIPAA Standards (OHS). Complaints may be filed electronically through the use of the ASET system which is accessed through the CMS website at http://www.cms.hhs.gov/hipaa/hipaa2, or directly at http://htct.hhs.gov or complaints can be filed in writing to OHS at: The Centers for Medicare and Medicaid Services HIPAA TCS Enforcement Activities / Complaint submission P.O. Box 8030 Baltimore, Maryland 21244-8030
261485	How do I file a HIPAA transaction and/or complaint electronically?	A HIPAA electronic transaction and/or code set complaint can be filed electronically by using the ASET online electronic compliance tool. This Internet based system enables individuals or organizations to file a complaint against an entity whose actions directly impact the ability of a HIPAA transaction to be accepted and/or efficiently processed. To file a transaction and/or code set complaint, ASET may be accessed through the CMS website at http://www.cms.hhs.gov/hipaa/hipaa2, or directly at http://htct.hhs.gov. When using ASET it is important to read all the information contained in the first few screens. This information will help determine whether the ASET system can be used to file a HIPAA complaint. When filing a complaint online, users will receive a username and password. The username and password are used to review the status of the complaint at anytime by logging on to the system. If users have further questions about a complaint that was submitted, they may also email OHS at HIPAAComplaint@cms.hhs.gov.
261586	What if I have problems using the ASET tool?	Any problems using the system should be referred to the email address within the "Technical Problems/Questions" link located on the first screen. A specialist will follow up to resolve the problem. For general questions about the complaint process, or to determine if a complaint is valid, email OHS at HIPAAComplaint@cms.hhs.gov.
261687	How do I file a transaction and/or code set complaint in writing?	Complaints may be submitted in writing to the Office of HIPAA Standards (OHS.) Written complaints require additional processing time to allow for mail and administrative time. Be sure to include: 1. Complainant name 2. Complainant organization 3. Complainant contact information 4. The name, address and telephone number of the entity the complainant is filing a compliant against 5. A description of the complaint

		The complaint form is available for download from the CMS website at http://www.cms.hhs.gov/hipaa/hipaa2. Mail all written complaints to: The Centers for Medicare and Medicaid Services HIPAA TCS Enforcement Activities/complaint submission P.O. Box 8030 Baltimore, Maryland 21244-8030 When OHS receives a complaint, an OHS representative will contact the complainant.
261788	Can I file a complaint against my software vendor?	The Office of HIPAA Standards (OHS) does not accept complaints filed against software vendors. Vendors are not covered entities under HIPAA and, therefore, OHS has no authority to investigate this type of complaint. Entities are encouraged to continue to work with software vendors to find solutions to any HIPAA transactions issues.
261889	What is OHS' privacy policy regarding information collected during the complaint process?	OHS has detailed privacy and security policies that explain how information is collected and stored when you file a complaint electronically or in writing. In general, OHS uses and discloses the relevant information contained in the written complaint form, through correspondence by mail, and through the online ASET system, only to resolve complaints that relate exclusively to violations of the HIPAA Transactions and Code Sets Rule. Before a complainant can submit a complaint against another entity, OHS requires that the complainant read and acknowledge the policies. The policies can be found on the ASET website (http://htct.hhs.gov) and in the paper complaint form which can be downloaded from the CMS website at http://www.cms.hhs.gov/hipaa/hipaa2. If complainants do not have access to the Internet, they may request copies of the complaint form (and privacy policy) by mail. Send requests for complaint forms to: The Centers for Medicare and Medicaid Services HIPAA TCS Enforcement Activities / Complaint Form Request P.O. Box 8030 Baltimore, Maryland 21244-8030 The complaint form will be mailed to the name and address included in the request.
261990	What is the standard that was adopted as the unique health identifier for health care providers?	The National Provider Identifier (NPI) was adopted as the standard unique health identifier for health care providers to carry out a requirement in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) for the adoption of such a standard. The NPI did not exist previously; it was developed as the unique identifier for health care providers because no existing standard met the criteria required of a national standard.
262091	What is the format of the NPI?	The National Provider Identifier (NPI) is all numeric and is 10 positions in length: the first 9 positions are the identifier and the last position is a check digit. The check digit helps detect invalid NPIs. There is no embedded intelligence in the NPI with respect to the health care provider that it identifies.
262192	Who is eligible to receive an NPI?	Entities who meet the definition of "health care provider", as defined at 45 C.F.R. § 160.103, are eligible to receive National Provider Identifiers (NPIs). Health care providers include hospitals, nursing homes, durable medical equipment suppliers, clinical laboratories, pharmacies, and many other "institutional" type providers;

		physicians, dentists, pharmacists, nurses, and many other health care practitioners and professionals; group practices, health maintenance organizations, and others.
262293	Is a health care provider required to obtain an NPI?	Under the National Provider Identifier Regulation (that was published in the Federal Register on January 23, 2004), a health care provider who is a covered entity, as defined at 45 C.F.R. § 160.103, is required to obtain a National Provider Identifier (NPI) by May 23, 2007.
262394	What is the purpose of the NPI? Who must use it, and when?	The purpose of the National Provider Identifier (NPI) is to uniquely identify a health care provider in standard transactions, such as health care claims. NPIs may also be used to identify health care providers on prescriptions, in internal files to link proprietary provider identification numbers and other information, in coordination of benefits between health plans, in patient medical record systems, in program integrity files, and in other ways. HIPAA requires that covered entities (i.e., health plans, health care clearinghouses, and those health care providers who transmit any health information in electronic form in connection with a transaction for which the Secretary of Health and Human Services has adopted a standard) use NPIs in standard transactions by the compliance dates. The compliance date for all covered entities except small health plans is May 23, 2007; the compliance date for small health plans is May 23, 2008. As of the compliance dates, the NPI will be the only health care provider identifier that can be used for identification purposes in standard transactions by covered entities.
262495	Will a health care provider continue to use other numbers besides the NPI to identify itself in standard transactions after the compliance date?	Upon the compliance dates, only the National Provider Identifier (NPI) may be used for identification purposes for a health care provider in standard transactions; legacy identifiers (such as the Unique Physician Identification Number (UPIN), Medicaid Provider Number, Medicare Provider Number, and others) may not be used. Where a health care provider must be identified in standard transactions for tax purposes, it would use its Taxpayer Identifying Number as required by the implementation specifications. Health care provider identification numbers other than the NPI may continue to be used in the internal processes and files of health plans or health care clearinghouses if they wish to continue to use those identification numbers in those internal processes and files.
262596	Who will assign NPIs to health care providers?	The Department of Health and Human Services will contract with an organization, known as the enumerator, to do this work. In addition to receiving and processing National Provider Identifier (NPI) applications and notifying health care providers of their NPIs, the enumerator will: use the National Provider System (NPS) to ensure the unique identification of a health care provider; answer questions about the processes of applying for and obtaining NPIs and furnishing updates; collect information, via the applications and updates, and maintain the NPS database containing NPIs and information about the health care providers to which they are assigned; and furnish information upon request and in accordance with established guidelines.
262697	How will a health care provider obtain an NPI?	A health care provider will obtain a National Provider Identifier (NPI) by submitting an application for an NPI—either on paper through the postal service or electronically over the Internet. After the application is successfully processed, the health care provider will be notified of its NPI. The CMS web site (www.cms.hhs.gov/hipaa/hipaa2) will contain information on when, where and how the NPI application can be obtained.

262798	When can a health care provider apply for an NPI?	Health care providers can apply for National Provider Identifiers (NPIs) beginning on the effective date of the final rule, which is May 23, 2005.
262899	How long will it take to get an NPI?	We cannot predict the amount of time it will take to obtain a National Provider Identifier (NPI) because several factors come into play. Such factors include the volume of applications being processed at a given time, whether the application was submitted electronically or on paper, and whether the application was complete and passed all edits. We expect that a health care provider who submits a properly completed electronic application could have its NPI in 10 days.
2629100	If a health care provider with an NPI moves to a new location, must the health care provider notify the enumerator of its new address?	A covered health care provider must notify the enumerator of changes in any of the information that it furnished on its application for a National Provider Identifier (NPI), and must do so within 30 days of the change. We encourage health care providers who have been assigned NPIs, but who are not covered entities, to do the same.
2630101	Will a health care provider's NPI ever change?	The National Provider Identifier (NPI) is meant to be a lasting identifier, and would not change based on changes in a health care provider's name, address, ownership, membership in health plans, or Healthcare Provider Taxonomy classification. There may be situations where use of an NPI for fraudulent purposes results in a health care provider requesting a different NPI; such situations will be investigated and a different NPI may be assigned to the requesting health care provider.
2631102	Will there be enough NPIs to enumerate all health care providers? Will we ever run out?	The format of the National Provider Identifier (NPI) and the assignment strategy will enable the enumeration of over 200 million health care providers. At the current rate of increase in the number of providers in the United States, this should enable the Department of Health and Human Services to enumerate health care providers for 200 years.
2632103	Will a health care provider continue to use other numbers besides the NPI to identify itself in standard transactions after the compliance date?	Upon the compliance dates, only the National Provider Identifier (NPI) may be used for identification purposes for a health care provider in standard transactions; legacy identifiers (such as the Unique Physician Identification Number (UPIN), Medicaid Provider Number, Medicare Provider Number, and others) may not be used. Where a health care provider must be identified in standard transactions for tax purposes, it would use its Taxpayer Identifying Number as required by the implementation specifications. Health care provider identification numbers other than the NPI may continue to be used in the internal processes and files of health plans or health care clearinghouses if they wish to continue to use those identification numbers in those internal processes and files.
2633103	Will there be a crosswalk of UPINs to NPIs?	The extract file that will be produced by the National Provider System will contain the information required for a UPIN crosswalk. The extract file may also include other health care provider identification numbers (such as Medicaid numbers and Drug Enforcement Administration (DEA) numbers) if those numbers were furnished by health care providers when they applied for NPIs.